ANNEX VI

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
OFFICE OF GENERAL COUNSEL
WASHINGTON, DC 20511

FEB 22 2016

Mr. Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Mr. Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Dear Mr. Antonipillai and Mr. Dean:

Over the last two and a half years, in the context of negotiations for the EU-U.S. Privacy Shield, the United States has provided substantial information about the operation of U.S. Intelligence Community signals intelligence collection activity. This has included information about the governing legal framework, the multi-layered oversight of those activities, the extensive transparency about those activities, and the overall protections for privacy and civil liberties, in order to assist the European Commission in making a determination about the adequacy of those protections as they relate to the national security exception to the Privacy Shield principles. This document summarizes the information that has been provided.

I. PPD-28 and the Conduct of U.S. Signals Intelligence Activity

The U.S. Intelligence Community collects foreign intelligence in a carefully controlled manner, in strict accordance with U.S. laws and subject to multiple layers of oversight, focusing on important foreign intelligence and national security priorities. A mosaic of laws and policies governs U.S. signals intelligence collection, including the U.S. Constitution, the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 *et seq.*) (FISA), Executive Order 12333 and its implementing procedures, Presidential guidance, and numerous procedures and guidelines, approved by the FISA Court and the Attorney General, that establish additional rules limiting the collection, retention, use, and dissemination of foreign intelligence information.[1]

a. PPD 28 Overview

In January 2014, President Obama gave a speech outlining various reforms to U.S. signals intelligence activities, and issued Presidential Policy Directive 28 (PPD-28) concerning

---

[1] Further information concerning U.S. foreign intelligence activities is posted online and publicly accessible through IC on the Record (www.icontherecord.tumblr.com), the ODNI's public website dedicated to fostering greater public visibility into the intelligence activities of the government.

those activities.[2] The President emphasized that U.S. signals intelligence activities help secure not only our country and our freedoms, but also the security and freedoms of other countries, including EU Member States, that rely on the information U.S. intelligence agencies obtain to protect their own citizens.

PPD-28 sets out a series of principles and requirements that apply to all U.S. signals intelligence activities and for all people, regardless of nationality or location. In particular, it sets certain requirements for procedures to address the collection, retention, and dissemination of personal information about non-U.S. persons acquired pursuant to U.S. signals intelligence. These requirements are set forth in more detail below, but in summary:

- The PPD reiterates that the United States collects signals intelligence only as authorized by statute, executive order, or other Presidential directive.
- The PPD establishes procedures to ensure that signals intelligence activity is conducted only in furtherance of legitimate and authorized national security purposes.
- The PPD also requires that privacy and civil liberties be integral concerns in the planning of signals intelligence collection activities. In particular, the United States does not collect intelligence to suppress or burden criticism or dissent; in order to disadvantage persons based on their ethnicity, race, gender, sexual orientation, or religion; or to afford a competitive commercial advantage to U.S. companies and U.S. business sectors.
- The PPD directs that signals intelligence collection be as tailored as feasible and that signals intelligence collected in bulk can only be used for specific enumerated purposes.
- The PPD directs that the Intelligence Community adopt procedures "reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities," and in particular extending certain protections afforded to the personal information of U.S. persons to non-US person information.
- Agency procedures implementing PPD-28 have been adopted and made public.

The applicability of the procedures and protections set out herein to the Privacy Shield is clear. When data has been transferred to corporations in the United States pursuant to the Privacy Shield, or indeed by any means, U.S. intelligence agencies can seek that data from those corporations only if the request complies with FISA or is made pursuant to one of the National Security Letter statutory provisions, which are discussed below.[3] In addition, without confirming or denying media reports alleging that the U.S. Intelligence Community collects data from transatlantic cables while it is being transmitted to the United States, were the U.S. Intelligence Community to collect data from transatlantic cables, it would do so subject to the limitations and safeguards set out herein, including the requirements of PPD-28.

b. Collection Limitations

PPD-28 sets out a number of important general principles that govern the collection of signals intelligence:

---

[2] *Available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[3] Law enforcement or regulatory agencies may request information from corporations for investigative purposes in the United States pursuant to other criminal, civil, and regulatory authorities that are beyond the scope of this paper, which is limited to national security authorities.

- The collection of signals intelligence must be authorized by statute or Presidential authorization, and must be undertaken in accordance with the Constitution and law.
- Privacy and civil liberties must be integral considerations in planning signals intelligence activities.
- Signals intelligence will be collected only when there is a valid foreign intelligence or counterintelligence purpose.
- The United States will not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent.
- The United States will not collect signals intelligence to disadvantage people based on their ethnicity, race, gender, sexual orientation, or religion.
- The United States will not collect signals intelligence to afford a competitive commercial advantage to U.S. companies and business sectors.
- U.S. signals intelligence activity must *always* be as tailored as feasible, taking into account the availability of other sources of information. This means, among other things, that whenever practicable, signals intelligence collection activities are conducted in a targeted manner rather than in bulk.

The requirement that signals intelligence activity be "as tailored as feasible" applies to the manner in which signals intelligence is collected, as well as to what is actually collected. For example, in determining whether to collect signals intelligence, the Intelligence Community must consider the availability of other information, including diplomatic or public sources, and prioritize collection through those means, where appropriate and feasible. Moreover, Intelligence Community element policies should require that wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (*e.g.*, specific facilities, selection terms and identifiers).

It is important to view the information provided to the Commission as a whole. Decisions about what is "feasible" or "practicable" are not left to the discretion of individuals but are subject to the policies that agencies have issued under PPD-28 – which have been made publicly available – and to the other processes described therein.[4] As PPD-28 says, bulk collection of signals intelligence is collection that "due to technical or operational considerations, is acquired without the use of discriminants (*e.g.*, specific identifiers, selection terms, etc.)." In this respect, PPD-28 recognizes that Intelligence Community elements must collect bulk signals intelligence in certain circumstances in order to identify new or emerging threats and other vital national security information that is often hidden within the large and complex system of modern global communications. It also recognizes the privacy and civil liberties concerns raised when bulk signals intelligence is collected. PPD-28 therefore directs the Intelligence Community to prioritize alternatives that would allow the conduct of targeted signals intelligence rather than bulk signals intelligence collection. Accordingly, Intelligence Community elements should conduct targeted signals intelligence collection activities rather than bulk signal intelligence

[4] *Available at* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. These procedures implement the targeting and tailoring concepts discussed in this letter in a manner specific to each IC element.

collection activities whenever practicable.[5] These principles ensure that the exception for bulk collection will not swallow the general rule.

As for the concept of "reasonableness," it is a bedrock principle of U.S. law. It signifies that Intelligence Community elements will not be required to adopt any measure theoretically possible, but rather will have to balance their efforts to protect legitimate privacy and civil liberties interests with the practical necessities of signals intelligence activities. Here again, the agencies' policies have been made available, and can provide assurance that the term "reasonably designed to minimize the dissemination and retention of personal information" does not undermine the general rule.

PPD-28 also provides that signals intelligence collected in bulk can only be used for six specific purposes: detecting and countering certain activities of foreign powers; counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to U.S. or allied armed forces; and combating transnational criminal threats, including sanctions evasion. The President's National Security Advisor, in consultation with the Director for National Intelligence (DNI), will annually review these permissible uses of signals intelligence collected in bulk to see whether they should be changed. The DNI will make this list publicly available to the maximum extent feasible, consistent with national security. This provides an important and transparent limitation on the use of bulk signals intelligence collection.

Additionally, the Intelligence Community elements implementing PPD-28 have reinforced existing analytic practices and standards for querying unevaluated signals intelligence.[6] Analysts must structure their queries or other search terms and techniques to ensure that they are appropriate to identify intelligence information relevant to a valid foreign intelligence or law enforcement task. To that end, IC elements must focus queries about persons on the categories of signals intelligence information responsive to a foreign intelligence or law enforcement requirement, so as to prevent the use of personal information not pertinent to foreign intelligence or law enforcement requirements.

It is important to emphasize that any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet. Additionally, the use of targeted queries, as described above, ensures that only those items believed to be of potential intelligence value are ever presented for analysts to examine. These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside.

The United States has elaborate processes to ensure that signals intelligence activities are conducted only in furtherance of appropriate national security purposes. Each year the President sets the nation's highest priorities for foreign intelligence collection after an extensive, formal interagency process. The DNI is responsible for translating these intelligence priorities into the

---

[5] To cite but one example, the NSA's procedures implementing PPD-28 state that "[w]henever practicable, collection will occur through the use of one or more selection terms in order to focus the collection on specific foreign intelligence targets (*e.g.*, a specific, known international terrorist or terrorist group) or specific foreign intelligence topics (*e.g.*, the proliferation of weapons of mass destruction by a foreign power or its agents)."

[6] *Available at* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

National Intelligence Priorities Framework, or NIPF. PPD-28 strengthened and enhanced the interagency process to ensure that all of the IC's intelligence priorities are reviewed and approved by high-level policymakers. Intelligence Community Directive (ICD) 204 provides further guidance on the NIPF and was updated in January 2015 to incorporate the requirements of PPD-28.[7] Although the NIPF is classified, information related to specific U.S. foreign intelligence priorities is reflected annually in the DNI's unclassified *Worldwide Threat Assessment*, which is also readily available on the ODNI website.

The priorities in the NIPF are at a fairly high level of generality. They include topics such as the pursuit of nuclear and ballistic missile capabilities by particular foreign adversaries, the effects of drug cartel corruption, and human rights abuses in specific countries. And they apply not just to signals intelligence, but to all intelligence activities. The organization that is responsible for translating the priorities in the NIPF into actual signals intelligence collection is called the National Signals Intelligence Committee, or SIGCOM. It operates under the auspices of the Director of the National Security Agency (NSA), who is designated by Executive Order 12333 as the "functional manager for signals intelligence," responsible for overseeing and coordinating signals intelligence across the Intelligence Community under the oversight of both the Secretary of Defense and the DNI. The SIGCOM has representatives from all elements of the IC and, as the United States fully implements PPD-28, also will have full representation from other departments and agencies with a policy interest in signals intelligence.

All U.S. departments and agencies that are consumers of foreign intelligence submit their requests for collection to the SIGCOM. The SIGCOM reviews those requests, ensures that they are consistent with the NIPF, and assigns them priorities using criteria such as:

- Can signals intelligence provide useful information in this case, or are there better or more cost-effective sources of information to address the requirement, such as imagery or open source information?
- How critical is this information need? If it is a high priority in the NIPF, it will most often be a high signal intelligence priority.
- What type of signals intelligence could be used?
- Is the collection as tailored as feasible? Should there be time, geographic, or other limitations?

The U.S. signals intelligence requirements process also requires explicit consideration of other factors, namely:

- Is the target of the collection, or the methodology used to collect, particularly sensitive? If so, it will require review by senior policymakers.
- Will the collection present an unwarranted risk to privacy and civil liberties, regardless of nationality?
- Are additional dissemination and retention safeguards necessary to protect privacy or national security interests?

---

[7] *Available at* http://www.dni.gov/files/documents/ICD/ICD%20204%20National %20Intelligence%20Priorities%20Framework.pdf.

Finally, at the end of the process, trained NSA personnel take the priorities validated by the SIGCOM and research and identify specific selection terms, such as telephone numbers or email addresses, which are expected to collect foreign intelligence responsive to these priorities. Any selector must be reviewed and approved before it is entered into NSA's collection systems. Even then, however, whether and when actual collection takes place will depend in part on additional considerations such as the availability of appropriate collection resources. This process ensures that U.S. signals intelligence collection targets reflect valid and important foreign intelligence needs. And, of course, when collection is conducted pursuant to FISA, NSA and other agencies must follow additional restrictions approved by the Foreign Intelligence Surveillance Court. In short, neither NSA nor any other U.S. intelligence agency decides on its own what to collect.

Overall, this process ensures that all U.S. intelligence priorities are set by senior policymakers who are in the best position to identify U.S. foreign intelligence requirements, and that those policymakers take into account not only the potential value of the intelligence collection but also the risks associated with that collection, including the risks to privacy, national economic interests, and foreign relations.

With respect to data transmitted to the United States pursuant to the Privacy Shield, although the United States cannot confirm or deny specific intelligence methods or operations, the requirements of PPD-28 apply to any signals intelligence operations the United States conducts, regardless of the type or source of data that is being collected. Further, the limitations and safeguards applicable to the collection of signals intelligence apply to signals intelligence collected for any authorized purpose, including both foreign relations and national security purposes.

The procedures discussed above demonstrate a clear commitment to prevent arbitrary and indiscriminate collection of signals intelligence information, and to implement – from the highest levels of our Government – the principle of reasonableness. PPD-28 and agency implementing procedures clarify new and existing limitations to and describe with greater specificity the purpose for which the United States collects and uses signals intelligence. These should provide assurance that signals intelligence activities are and will continue to be conducted only to further legitimate foreign intelligence goals.

c. __Retention and Dissemination Limitations__

Section 4 of PPD-28 requires that each element of the Intelligence Community have express limits on the retention and dissemination of personal information about non-U.S. persons collected by signals intelligence, comparable to the limits for U.S. persons. These rules are incorporated into procedures for each IC agency that were released in February 2015 and are publicly available. To qualify for retention or dissemination as foreign intelligence, personal information must relate to an authorized intelligence requirement, as determined in the NIPF process described above; be reasonably believed to be evidence of a crime; or meet one of the other standards for retention of U.S. person information identified in Executive Order 12333, section 2.3.

Information for which no such determination has been made may not be retained for more than five years, unless the DNI expressly determines that continued retention is in the national security interests of the United States. Thus, IC elements must delete non-U.S. person information collected through signals intelligence five years after collection, unless, for example, the information has been determined to be relevant to an authorized foreign intelligence requirement, or if the DNI determines, after considering the views of the ODNI Civil Liberties Protection Officer and agency privacy and civil liberties officials, that continued retention is in the interest of national security.

In addition, all agency policies implementing PPD-28 now explicitly require that information about a person may not be disseminated solely because an individual is a non-U.S. person, and ODNI has issued a directive to all IC elements[8] to reflect this requirement. Intelligence Community personnel are specifically required to consider the privacy interests of non-U.S. persons when drafting and disseminating intelligence reports. In particular, signals intelligence about the routine activities of a foreign person would not be considered foreign intelligence that could be disseminated or retained permanently by virtue of that fact alone unless it is otherwise responsive to an authorized foreign intelligence requirement. This recognizes an important limitation and is responsive to European Commission concerns about the breadth of the definition of foreign intelligence as set forth in Executive Order 12333.

d. Compliance and Oversight

The U.S. system of foreign intelligence oversight provides rigorous and multi-layered oversight to ensure compliance with applicable laws and procedures, including those pertaining to the collection, retention, and dissemination of non-U.S. person information acquired by signals intelligence as set forth in PPD-28. These include:

- The Intelligence Community employs hundreds of oversight personnel. NSA alone has over 300 people dedicated to compliance, and other elements also have oversight offices. In addition, the Department of Justice provides extensive oversight of intelligence activities, and oversight is also provided by the Department of Defense.
- Each element of the Intelligence Community has its own Office of the Inspector General with responsibility for oversight of foreign intelligence activities, among other matters. Inspectors General are statutorily independent; have broad power to conduct investigations, audits and reviews of programs, including of fraud and abuse or violation of law; and can recommend corrective actions. While Inspector General recommendations are non-binding, the Inspector General's reports are often made public, and in any event are provided to Congress; this includes follow-up reports in case corrective action recommended in previous reports has not yet been completed. Congress is therefore informed of any non-compliance and can exert pressure, including through budgetary means, to achieve corrective action. A number of Inspector General reports about intelligence programs have been publicly released.[9]

---

[8] Intelligence Community Directive (ICD) 203, *available at* http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

[9] *See, e.g.*, U.S. Department of Justice Inspector General Report "A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008" (September 2012), *available at* https://oig.justice.gov/reports/2016/o1601a.pdf.

- ODNI's Civil Liberties and Privacy Office (CLPO) is charged with ensuring that the IC operates in a manner that advances national security while protecting civil liberties and privacy rights.[10] Other IC elements have their own privacy officers.
- The Privacy and Civil Liberties Oversight Board (PCLOB), an independent body established by statute, is charged with analyzing and reviewing counterterrorism programs and policies, including the use of signals intelligence, to ensure that they adequately protect privacy and civil liberties. It has issued several public reports on intelligence activities.
- As discussed more fully below, the Foreign Intelligence Surveillance Court, a court composed of independent federal judges, is responsible for oversight and compliance of any signals intelligence collection activities conducted pursuant to FISA.
- Finally, the U.S. Congress, specifically the House and Senate Intelligence and Judiciary Committees, have significant oversight responsibilities regarding all U.S. foreign intelligence activities, including U.S. signals intelligence.

Apart from these formal oversight mechanisms, the Intelligence Community has in place numerous mechanisms to ensure that the Intelligence Community is complying with the limitations on collection described above. For example:

- Cabinet officials are required to validate their signals intelligence requirements each year.
- NSA checks signals intelligence targets throughout the collection process to determine if they are actually providing valuable foreign intelligence responsive to the priorities, and will stop collection against targets that are not. Additional procedures ensure that selection terms are reviewed periodically.
- Based on a recommendation from an independent Review Group appointed by President Obama, the DNI has established a new mechanism to monitor the collection and dissemination of signals intelligence that is particularly sensitive because of the nature of the target or the means of collection, to ensure that it is consistent with the determinations of policymakers.
- Finally, ODNI annually reviews the IC's allocation of resources against the NIPF priorities and the intelligence mission as a whole. This review includes assessments of the value of all types of intelligence collection, including signals intelligence, and looks both backward – how successful has the IC been in achieving its goals? – and forward – what will the IC need in the future? This ensures that signals intelligence resources are applied to the most important national priorities.

As evidenced by this comprehensive overview, the Intelligence Community does not decide on its own which conversations to listen to, try to collect everything, or operate free from scrutiny. Its activities are focused on priorities set by policymakers, through a process that involves input from across the government, and that is overseen both within NSA and by the ODNI, Department of Justice, and Department of Defense.

PPD-28 also contains numerous other provisions to ensure that personal information collected pursuant to signals intelligence is protected, regardless of nationality. For instance,

[10] *See* www.dni.gov/clpo.

PPD-28 provides for data security, access, and quality procedures to protect personal information collected through signals intelligence, and provides for mandatory training to ensure that the workforce understands the responsibility to protect personal information, regardless of nationality. The PPD also provides for additional oversight and compliance mechanisms. These include periodic audit and reviews by appropriate oversight and compliance officials of the practices for protecting personal information contained in signals intelligence. The reviews also must examine the agencies' compliance with the procedures for protecting such information.

Additionally, PPD-28 provides that significant compliance issues related to non-U.S. persons will be addressed at senior levels of government. Should a significant compliance issue occur involving the personal information of any person collected as a result of signals intelligence activities, the issue must, in addition to any existing reporting requirements, be reported promptly to the DNI. If the issue involves the personal information of a non-U.S. person, the DNI, in consultation with the Secretary of State and the head of the relevant IC element, will determine whether steps should be taken to notify the relevant foreign government, consistent with the protection of sources and methods and of U.S. personnel. Moreover, as directed by PPD-28, the Secretary of State has identified a senior official, Under Secretary Catherine Novelli, to serve as a point of contact for foreign governments that wish to raise concerns regarding signals intelligence activities of the United States. This commitment to high-level engagement exemplifies the efforts the U.S. government has made over the past few years to instill confidence in the numerous and overlapping privacy protections in place for U.S. person and non-U.S. person information.

e. ***Summary***

The United States' processes for collecting, retaining, and disseminating foreign intelligence provide important privacy protections for the personal information of all persons, regardless of nationality. In particular, these processes ensure that our Intelligence Community focuses on its national security mission as authorized by applicable laws, executive orders, and presidential directives; safeguards information from unauthorized access, use and disclosure; and conducts its activities under multiple layers of review and oversight, including by congressional oversight committees. PPD-28 and the procedures implementing it represent our efforts to extend certain minimization and other substantial data protection principles to the personal information of all persons regardless of nationality. Personal information obtained through U.S. signals intelligence collection is subject to the principles and requirements of U.S. law and Presidential direction, including the protections set forth in PPD-28. These principles and requirements ensure that all persons are treated with dignity and respect, regardless of their nationality or wherever they might reside, and recognize that all persons have legitimate privacy interests in the handling of their personal information.

II. <u>Foreign Intelligence Surveillance Act – Section 702</u>

Collection under Section 702 of the Foreign Intelligence Surveillance Act[11] is not "mass and indiscriminate" but is narrowly focused on the collection of foreign intelligence from individually identified legitimate targets; is clearly authorized by explicit statutory authority; and is subject to both independent judicial supervision and substantial review and oversight within

[11] 50 U.S.C. § 1881a.

the Executive Branch and Congress. Collection under Section 702 is considered signals intelligence subject to the requirements of PPD-28.[12]

Collection under Section 702 is one of the most valuable sources of intelligence protecting both the United States and our European partners. Extensive information about the operation and oversight of Section 702 is publicly available. Numerous court filings, judicial decisions and oversight reports relating to the program have been declassified and released on the ODNI's public disclosure website, www.icontherecord.tumblr.com. Moreover, Section 702 was comprehensively analyzed by the PCLOB, in a report which is available at https://www.pclob.gov/library/702-Report.pdf.[13]

Section 702 was passed as part of the FISA Amendments Act of 2008,[14] after extensive public debate in Congress. It authorizes the acquisition of foreign intelligence information through targeting of non-U.S. persons located outside the United States, with the compelled assistance of U.S. electronic communications service providers. Section 702 authorizes the Attorney General and the DNI – two Cabinet-level officials appointed by the President and confirmed by the Senate – to submit annual certifications to the FISA Court.[15] These certifications identify specific categories of foreign intelligence to be collected, such as intelligence related to counterterrorism or weapons of mass destruction, which must fall within the categories of foreign intelligence defined by the FISA statute.[16] As the PCLOB noted, "[t]hese limitations do *not* permit unrestricted collection of information about foreigners."[17]

The certifications also are required to include "targeting" and "minimization" procedures that must be reviewed and approved by the FISA Court.[18] The targeting procedures are designed to ensure that the collection takes place only as authorized by statute and is within the scope of the certifications; the minimization procedures are designed to limit the acquisition, dissemination, and retention of information about U.S. persons, but also contain provisions that provide substantial protection to information about non-U.S. persons as well, as described below. Moreover, as described above, in PPD-28 the President directed that the Intelligence Community

[12] The United States also may obtain court orders pursuant to other provisions of FISA for the production of data, including data transferred pursuant to the Privacy Shield. *See* 50 U.S.C. § 1801 *et seq*. Titles I and III of FISA, which respectively authorize electronic surveillance and physical searches, require a court order (except in emergency circumstances) and always require probable cause to believe that the target is a foreign power or an agent of a foreign power. Title IV of FISA authorizes the use of pen registers and trap and trace devices, pursuant to court order (except in emergency circumstances) in authorized foreign intelligence, counterintelligence, or counterterrorism investigations. Title V of FISA permits the FBI, pursuant to court order (except in emergency circumstances), to obtain business records that are relevant to an authorized foreign intelligence, counterintelligence, or counterterrorism investigations. As discussed below, the USA FREEDOM Act specifically prohibits the use of FISA pen register or business record orders for bulk collection, and imposes a requirement of a "specific selection term" to ensure that those authorities are used in a targeted fashion.

[13] Privacy and Civil Liberties Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (July 2, 2014) ("PCLOB Report").

[14] *See* Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[15] *See* 50 U.S.C. § 1881a(a) and (b).

[16] *See id.* § 1801(e).

[17] *See* PCLOB Report at 99.

[18] *See* 50 U.S.C. § 1881a(d) and (e).

provide additional protections for personal information about non-U.S. persons, and those protections apply to information collected under Section 702.

Once the court approves the targeting and minimization procedures, collection under Section 702 is not bulk or indiscriminate, but "consists entirely of targeting specific persons about whom an individualized determination has been made," as the PCLOB said.[19] Collection is targeted through the use of individual selectors, such as email addresses or telephone numbers, which U.S. intelligence personnel have determined are likely being used to communicate foreign intelligence information of the type covered by the certification submitted to the court.[20] The basis for selection of the target must be documented, and the documentation for every selector is subsequently reviewed by the Department of Justice.[21] The U.S. Government has released information showing that in 2014 there were approximately 90,000 individuals targeted under Section 702, a miniscule fraction of the over 3 billion internet users throughout the world.[22]

Information collected under Section 702 is subject to the court-approved minimization procedures, which provide protections to non-U.S. persons as well as U.S. persons, and which have been publicly released.[23] For example, communications acquired under Section 702, whether of U.S. persons or non-U.S. persons, are stored in databases with strict access controls. They may be reviewed only by intelligence personnel who have been trained in the privacy-protective minimization procedures and who have been specifically approved for that access in order to carry out their authorized functions.[24] Use of the data is limited to identification of foreign intelligence information or evidence of a crime.[25] Pursuant to PPD-28, this information may be disseminated only if there is a valid foreign intelligence or law enforcement purpose; the mere fact that one party to the communication is not a U.S. person is not sufficient.[26] And the minimization procedures and PPD-28 also set limits on how long data acquired pursuant to Section 702 may be retained.[27]

Oversight of Section 702 is extensive, and is conducted by all three branches of our government. Agencies implementing the statute have multiple levels of internal review, including by independent Inspectors General, and technological controls over access to the data. The Department of Justice and the ODNI closely review and scrutinize the use of Section 702 to verify compliance with legal rules; agencies are also under an independent obligation to report

---

[19] *See* PCLOB Report at 111.
[20] *Id.*
[21] *Id.* at 8; 50 U.S.C. § 1881a(l); *see also* NSA Director of Civil Liberties and Privacy Report, "NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" (hereinafter "NSA Report") at 4, *available at* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[22] Director of National Intelligence 2014 Transparency Report, *available at* www.icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.
[23] Minimization procedures available at: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf ("NSA Minimization Procedures"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd 28/2014%20CIA%20702%20Minimization%20Procedures.pdf.
[24] *See* NSA Report at 4.
[25] *See, e.g.,* NSA Minimization Procedures at 6.
[26] Intelligence Agency PPD-28 procedures available at www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[27] *See* NSA Minimization Procedures; PPD-28 Section 4.

potential incidents of noncompliance. Those incidents are investigated, and all compliance incidents are reported to the Foreign Intelligence Surveillance Court, the President's Intelligence Oversight Board, and Congress, and remedied as appropriate. [28] To date, there have been no incidents of willful attempts to violate the law or circumvent legal requirements. [29]

The FISA Court plays an important role in implementing Section 702. It is composed of independent federal judges who serve for a term of seven years on the FISA Court but who, like all federal judges, have life tenure as judges. As noted above, the Court must review the annual certifications and targeting and minimization procedures for compliance with the law. In addition, as also noted above, the Government is required to notify the Court immediately of compliance issues,[30] and several Court opinions have been declassified and released showing the exceptional degree of judicial scrutiny and independence it exercises in reviewing those incidents.

The Court's exacting processes have been described by its former Presiding Judge in a letter to Congress that has been publicly released.[31] And as a result of the USA FREEDOM Act, described below, the Court is now explicitly authorized to appoint an outside lawyer as an independent advocate on behalf of privacy in cases that present novel or significant legal issues.[32] This degree of involvement by a country's independent judiciary in foreign intelligence activities directed at persons who are neither citizens of that country nor located within it is unusual if not unprecedented, and helps ensure that Section 702 collection occurs within appropriate legal limits.

Congress exercises oversight through statutorily required reports to the Intelligence and Judiciary Committees, and frequent briefings and hearings. These include a semiannual report by the Attorney General documenting the use of Section 702 and any compliance incidents; [33] a separate semiannual assessment by the Attorney General and the DNI documenting compliance with the targeting and minimization procedures, including compliance with the procedures designed to ensure that collection is for a valid foreign intelligence purpose;[34] and an annual report by heads of intelligence elements which includes a certification that collection under Section 702 continues to produce foreign intelligence information.[35]

In short, collection under Section 702 is authorized by law; is subject to multiple levels of review, judicial supervision and oversight; and, as the FISA Court stated in a recently

[28] *See* 50 U.S.C. § 1881(l); *see also* PCLOB Report at 66-76.
[29] *See* Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence at 2-3, *available at* http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.
[30] Rule 13 of the Foreign Intelligence Surveillance Court Rules of Procedures, *available at* http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.
[31] July 29, 2013 Letter from The Honorable Reggie B. Walton to The Honorable Patrick J. Leahy, *available at* http://fas.org/irp/news/2013/07/fisc-leahy.pdf.
[32] *See* Section 401 of the USA FREEDOM Act, P.L. 114-23.
[33] *See* 50 U.S.C. § 1881f.
[34] *See id.* § 1881a(l)(1).
[35] *See id.* § 1881a(l)(3). Some of these reports are classified.

declassified opinion, is "not conducted in a bulk or indiscriminate manner," but "through . . . discrete targeting decisions for individual [communication] facilities."[36]

III. USA FREEDOM Act

The USA FREEDOM Act, signed into law in June 2015, significantly modified U.S. surveillance and other national security authorities, and increased public transparency on the use of these authorities and on decisions of the FISA Court, as set out below.[37] The Act ensures that our intelligence and law enforcement professionals have the authorities they need to protect the Nation, while further ensuring that individuals' privacy is appropriately protected when these authorities are employed. It enhances privacy and civil liberties and increases transparency.

The Act prohibits bulk collection of any records, including of both U.S. and non-U.S. persons, pursuant to various provisions of FISA or through the use of National Security Letters, a form of statutorily authorized administrative subpoenas.[38] This prohibition specifically includes telephone metadata relating to calls between persons inside the U.S. and persons outside the U.S., and would also include collection of Privacy Shield information pursuant to these authorities. The Act requires that the government base any application for records under those authorities on a "specific selection term"—a term that specifically identifies a person, account, address, or personal device in a way that limits the scope of information sought to the greatest extent reasonably practicable.[39] This further ensures that collection of information for intelligence purposes is precisely focused and targeted.

The Act also made significant modifications to proceedings before the FISA Court, which both increase transparency and provide additional assurances that privacy will be protected. As noted above, it authorized creation of a standing panel of security-cleared lawyers with expertise in privacy and civil liberties, intelligence collection, communications technology, or other relevant areas, who may be appointed to appear before the court as *amicus curiae* in cases that involve significant or novel interpretations of law. These lawyers are authorized to make legal arguments that advance the protection of individual privacy and civil liberties, and will have access to any information, including classified information, that the court determines is necessary to their duties.[40]

---

[36] Mem. Opinion and Order at 26 (FISC 2014), *available at* http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

[37] *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268.

[38] *See id.* §§ 103, 201, 501. National Security Letters are authorized by a variety of statutes and allow the FBI to obtain information contained in credit reports, financial records, and electronic subscriber and transaction records from certain kinds of companies, only to protect against international terrorism or clandestine intelligence activities. *See* 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. National Security Letters are typically used by the FBI to gather critical non-content information at the early phases of counterterrorism and counterintelligence investigations – such as the identity of the subscriber to an account who may have been communicating with agents of a terrorist group such as ISIL. Recipients of a National Security Letter have the right to challenge them in court. *See* 18 U.S.C. § 3511.

[39] *See* USA FREEDOM Act § 107.

[40] *See id.* § 401.

The Act also builds on the U.S. Government's unprecedented transparency about intelligence activities by requiring the DNI, in consultation with the Attorney General, to either declassify, or publish an unclassified summary of, each decision, order, or opinion issued by the FISA Court or the Foreign Intelligence Surveillance Court of Review that includes a significant construction or interpretation of any provision of law.

Moreover, the Act provides for extensive disclosures about FISA collection and National Security Letter requests. The United States must disclose to Congress and to the public each year the number of FISA orders and certifications sought and received; estimates of the number of U.S. persons and non-U.S. persons targeted and affected by surveillance; and the number of appointments of *amici curiae*, among other items of information.[41] The Act also requires additional public reporting by the government about the numbers of National Security Letter requests about both U.S. and non-U.S. persons.[42]

With regard to corporate transparency, the Act gives companies a range of options to report publicly the aggregate number of FISA orders and directives or National Security Letters they receive from the Government, as well as the number of customer accounts targeted by these orders.[43] Several companies have already made such disclosures, which have revealed the limited number of customers whose records have been sought.

These corporate transparency reports demonstrate that U.S. intelligence requests affect only a miniscule fraction of data. For example, one major company's recent transparency report shows that it received national security requests (pursuant to FISA or National Security Letters) affecting fewer than 20,000 of its accounts, at a time when it had at least 400 million subscribers. In other words, all U.S. national security requests reported by this company affected fewer than .005% of its subscribers. Even if every one of those requests had concerned Safe Harbor data, which of course is not the case, it is obvious that the requests are targeted and appropriate in scale, and are neither bulk nor indiscriminate.

Finally, while the statutes which authorize National Security Letters already restricted the circumstances under which a recipient of such a letter could be barred from disclosing it, the Act further provided that such non-disclosure requirements must be reviewed periodically; required that recipients of National Security Letters be notified when the facts no longer support a non-disclosure requirement; and codified procedures for recipients to challenge nondisclosure requirements.[44]

In sum, the USA FREEDOM Act's important amendments to U.S. intelligence authorities are clear evidence of the extensive effort taken by the United States to place the protection of personal information, privacy, civil liberties, and transparency at the forefront of all U.S. intelligence practices.

---

41 *See id.* § 602.
42 *See id.*
43 *See id.* § 603.
44 *See id.* §§ 502, 503.

IV. Transparency

In addition to the transparency mandated by the USA FREEDOM Act, the U.S. Intelligence Community provides the public much additional information, setting a strong example with respect to transparency into its intelligence activities. The Intelligence Community has published many of its policies, procedures, Foreign Intelligence Surveillance Court decisions, and other declassified materials, providing an extraordinary degree of transparency. In addition, the Intelligence Community has substantially increased its disclosure of statistics on the government's use of national security collection authorities. On April 22, 2015, the Intelligence Community issued its second annual report presenting statistics on how often the government uses these important authorities. ODNI also has published, on the ODNI website and on *IC On the Record*, a set of concrete transparency principles[45] and an implementation plan that translates the principles into concrete, measurable initiatives.[46] In October 2015, the Director of National Intelligence directed that each intelligence agency designate an Intelligence Transparency Officer within its leadership to foster transparency and lead transparency initiatives.[47] The Transparency Officer will work closely with each intelligence agency's Privacy and Civil Liberties Officer to ensure that transparency, privacy, and civil liberties continue to remain top priorities.

As an example of these efforts, NSA's Chief Privacy and Civil Liberties Officer has released several unclassified reports over the past few years, including reports on activities under section 702, Executive Order 12333, and the USA FREEDOM Act.[48] In addition, the IC works closely with the PCLOB, Congress, and the U.S. privacy advocacy community to provide further transparency relating to U.S. intelligence activities, wherever feasible and consistent with the protection of sensitive intelligence sources and methods. Taken as a whole, U.S. intelligence activities are as transparent as or more transparent than those of any other nation in the world and are as transparent as it is possible to be consistent with the need to protect sensitive sources and methods.

To summarize the extensive transparency that exists about U.S. intelligence activities:

- The IC has released and posted online thousands of pages of court opinions and agency procedures outlining the specific procedures and requirements of our intelligence activities. We have also released reports on intelligence agencies' compliance with applicable restrictions.
- Senior intelligence officials regularly speak publicly about the roles and activities of their organizations, including descriptions of the compliance regimes and safeguards that govern their work.

---

[45] *Available at* http:\\www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.

[46] *Available at* http:\\www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.

[47] *See id.*

[48] *Available at* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

- The IC released numerous additional documents about intelligence activities pursuant to our Freedom of Information Act.
- The President issued PPD-28, publicly setting out additional restrictions on our intelligence activities, and ODNI has issued two public reports on the implementation of those restrictions.
- The IC is now required by law to release significant legal opinions issued by the FISA Court, or summaries of those opinions.
- The government is required to report annually on the extent of its use of certain national security authorities, and companies are authorized to do so as well.
- The PCLOB has issued several detailed public reports on intelligence activities, and will continue to do so.
- The IC provides extensive classified information to Congressional oversight committees.
- The DNI issued transparency principles to govern the activities of the Intelligence Community.

This extensive transparency will continue going forward. Any information that is released publicly will, of course, be available to both the Department of Commerce and the European Commission. The annual review between Commerce and the European Commission on the implementation of the Privacy Shield will provide an opportunity for the European Commission to discuss any questions raised by any new information released, as well as any other matters concerning the Privacy Shield and its operation, and we understand that the Department may, in its discretion, invite representatives of other agencies, including the IC, to participate in that review. This is, of course, in addition to the mechanism provided in PPD-28 for EU Member States to raise surveillance-related concerns with a designated State Department official.

V. Redress

U.S. law provides a number of avenues of redress for individuals who have been the subject of unlawful electronic surveillance for national security purposes. Under FISA, the right to seek relief in U.S. court is not limited to U.S. persons. An individual who can establish standing to bring suit would have remedies to challenge unlawful electronic surveillance under FISA. For example, FISA allows persons subjected to unlawful electronic surveillance to sue U.S. government officials in their personal capacities for money damages, including punitive damages and attorney's fees. *See* 50 U.S.C. § 1810. Individuals who can establish their standing to sue also have a civil cause of action for money damages, including litigation costs, against the United States when information about them obtained in electronic surveillance under FISA has been unlawfully and willfully used or disclosed. *See* 18 U.S.C. § 2712. In the event the government intends to use or disclose any information obtained or derived from electronic surveillance of any aggrieved person under FISA against that person in judicial or administrative proceedings in the United States, it must provide advance notice of its intent to the tribunal and the person, who may then challenge the legality of the surveillance and seek to suppress the information. *See* 50 U.S.C. § 1806. Finally, FISA also provides criminal penalties for individuals who intentionally engage in unlawful electronic surveillance under color of law or who intentionally use or disclose information obtained by unlawful surveillance. *See* 50 U.S.C. § 1809.

EU citizens have other avenues to seek legal recourse against U.S. government officials for unlawful government use of or access to data, including government officials who violate the law in the course of unlawful access to or use of information for purported national security purposes. The Computer Fraud and Abuse Act prohibits intentional unauthorized access (or exceeding authorized access) to obtain information from a financial institution, a U.S. government computer system, or a computer accessed via the Internet, as well as threats to damage protected computers for purposes of extortion or fraud. *See* 18 U.S.C. § 1030. Any person, of whatever nationality, who suffers damage or loss by reason of a violation of this law may sue the violator (including a government official) for compensatory damages and injunctive or other equitable relief under section 1030(g), regardless of whether a criminal prosecution has been pursued, provided the conduct involves at least one of several circumstances set forth in the statute. The Electronic Communications Privacy Act (ECPA) regulates government access to stored electronic communications and transactional records and subscriber information held by third-party communications providers. *See* 18 U.S.C. §§ 2701-2712. ECPA authorizes an aggrieved individual to sue government officials for intentional unlawful access to stored data. ECPA applies to all persons regardless of citizenship and aggrieved persons may receive damages and attorney's fees. The Right to Financial Privacy Act (RFPA) limits the U.S. government's access to the bank and broker-dealer records of individual customers. *See* 12 U.S.C. §§ 3401-3422. Under the RFPA, a bank or broker-dealer customer can sue the U.S. government for statutory, actual, and punitive damages for wrongfully obtaining access to the customer's records, and a finding that such wrongful access was willful automatically triggers an investigation of possible disciplinary action against the relevant government employees. *See* 12 U.S.C. § 3417.

Finally, the Freedom of Information Act (FOIA) provides a means for any person to seek access to existing federal agency records on any topic subject to certain categories of exemptions. *See* 5 U.S.C. § 552(b). These include limits on access to classified national security information, personal information of other individuals and information concerning law enforcement investigations, and are comparable to the limitations imposed by nations with their own information access laws. These limitations apply equally to Americans and non-Americans. Disputes over the release of records requested pursuant to FOIA can be appealed administratively and then in federal court. The court is required to make a de novo determination of whether records are properly withheld, 5 U.S.C. § 552(a)(4)(B), and can compel the government to provide access to records. In some cases courts have overturned government assertions that information should be withheld as classified.[49] Although no monetary damages are available, courts can award attorney's fees.

VI. Conclusion

The United States recognizes that our signals intelligence and other intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or place of residence, and that all persons have legitimate privacy interests in the handling of their personal information. The United States only uses signals intelligence to advance its national security and foreign policy interests and to protect its citizens and the

[49] *See, e.g., New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

citizens of its allies and partners from harm. In short, the IC does not engage in indiscriminate surveillance of anyone, including ordinary European citizens. Signals intelligence collection only takes place when duly authorized and in a manner that strictly complies with these limitations; only after consideration of the availability of alternative sources, including from diplomatic and public sources; and in a manner that prioritizes appropriate and feasible alternatives. And wherever practicable, signals intelligence only takes place through collection focused on specific foreign intelligence targets or topics through the use of discriminants.

U.S. policy in this regard was affirmed in PPD-28. Within this framework, U.S. intelligence agencies do not have the legal authority, the resources, the technical capability or the desire to intercept all of the world's communications. Those agencies are not reading the emails of everyone in the United States, or of everyone in the world. Consistent with PPD-28, the United States provides robust protections to the personal information of non-U.S. persons that is collected through signals intelligence activities. To the maximum extent feasible consistent with the national security, this includes policies and procedures to minimize the retention and dissemination of personal information concerning non-U.S. persons comparable to the protections enjoyed by U.S. persons. Moreover, as discussed above, the comprehensive oversight regime of the targeted Section 702 FISA authority is unparalleled. Finally, the significant amendments to U.S. intelligence law set forth in the USA FREEDOM Act and the ODNI-led initiatives to promote transparency within the Intelligence Community greatly enhance the privacy and civil liberties of all individuals, regardless of their nationality.

Sincerely,

Robert S. Litt